УДК 004.056-047.44:336.71
DOI: 10.31673/2409-7292.2025.025553

Панаско О.М., Сагун А.В., Гавриш О.С.

АНАЛІЗ ТРЕНДІВ КІБЕРЗАГРОЗ ЯК ВАЖЛИВИЙ ЕТАП УПРАВЛІННЯ РИЗИКАМИ ФІНАНСОВОГО СЕКТОРУ

Аналіз кіберзагроз фінансового сектору актуалізує концепцію ризик-орієнтованого підходу в діяльності фінансових установ та дозволяє своєчасно реагувати на інциденти. Відстеження та розуміння трендів кіберзагроз сприяють ефективному управлінню кіберризиками. Для визначення вектору змін ландшафту загроз важливо враховувати досвід різних країн, щоб адаптувати найкращі практики до українських реалій. В умовах повномасштабної війни українські фінансові установи, зокрема банки, продемонстрували помітне зростання стійкості до кібератак. Набутий в таких складних умовах досвід дозволив банкам зміцнити технічні та організаційні можливості протидії інцидентам. Важливу роль у цьому відіграла скоординована взаємодія державних органів та приватних організацій, CERT-UA, діяльність спеціалізованих підрозділів України – Департаменту кіберполіції Національної поліції України, Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, управління захисту критичної інфраструктури НБУ, а також міжбанківське співробітництво у сфері обміну інформацією про загрози, міжнародна співпраця у сфері забезпечення кібербезпеки в банківському секторі. Такий підхід становить основу для підвищення швидкості реагування на кіберінциденти та сприятиме загальному посиленню кіберзахисту фінансового сектору України.

Ключові слова: ландшафт кіберзагроз фінансового сектору, кіберстійкість банків, кіберзлочинні організації, DDoS-атаки, CERT-UA, Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, НБУ, MISP-UA.

Вступ і формулювання проблеми

Фінансовий сектор відіграє ключову роль в економіці, забезпечуючи підтримку бізнесу, сприяючи інвестиціям в інфраструктуру, інноваціям, проведенню платежів для підтримки торгівлі, підтримуючи загальну макроекономічну стабільність через інструменти монетарної політики.

Технологічний прогрес та інновації в цій сфері підвищують її ефективність через зниження витрат та покращення фінансових послуг на прикладі застосування технологій фінтеху, блокчейн та цифрових валют. Цифровізація фінансової сфери надає переваги та підвищує конкурентоспроможність на основі можливостей штучного інтелекту для реалізація взаємодії з клієнтами через чат-боти з орієнтацією на кастомізацію користувацьких потреб. Водночас перехід до використання цифрових каналів та віддалених сервісів призводить до збільшення масштабів атак, появі нових векторів атак та впровадженню нових тактик та стратегій впливу. Яскравим прикладом слугують зафіксовані випадки використання штучного інтелекту, зокрема, великих мовних моделей LLM у шахрайських схемах в США, Канаді, Великій Британії [1].

Контекст повномасштабного вторгнення росії в Україну вніс корективи та ускладнив ландшафт кіберзагроз вітчизняної фінансової сфери та вплинув на сучасний світ. За дозволом НБУ на період дії воєнного стану було врегульовано можливість використання банками в своїй діяльності хмарних послуг. Сучасним банкам дозволено надавати послуги та керувати операціями за використання хмарних сервісів та обладнання, розміщеного на території США, Великої Британії, Канади та країн ЄС.

Використання хмарних технологій фінансовим сектором – це одночасно і виправдане стратегічне рішення, і потенційний виклик, пов'язаний з кібербезпекою. Через концентрацію значного спектру конфіденційної інформації на основі даних для обробки банківських операцій та персональних даних клієнтів, фінансові установи є привабливими для зловмисників, а їх ресурси – мішенями для кібератак.

У зв'язку з цим особливої уваги потребують нові підходи до управління кіберризиками внаслідок зростання кібератак та постійної зміни ландшафту кіберзагроз, оскільки розуміння кіберзагроз важливе не лише для захисту активів, а також для відповідності регуляторним вимогам та підтримки стабільності фінансової системи.

Аналіз літератури

Контекст цифровізації банківської сфери широко висвітлюється в публікаціях зарубіжних та вітчизняних авторів Forcadell F.J., Aracil E., Ubeda F., а також Карчевої І.Я., Кльоби Л.Г., Корнівської В.О. [2-5]. Сучасні процеси цифрової трансформації фінансової сфери нерозривно пов'язані з підвищенням конкурентноздатності, розширенням можливості провадити функціональну діяльність у наближенні до світових стандартів приватного життя клієнтів [6]. На думку автора [7] на найближчу перспективу прогнозовано зосередження уваги на технологіях і постійних інвестиціях в ІТ, а в роботі [8] досліджуються можливості інтеграції різноманітних аспектів FinTech в масштабах всього сектору. Обмеження технологічних та регуляторних аспектів застосування інноваційних рішень банківського сектору, а також складності адаптації інноваційних рішень з управлінськими обґрунтовано в роботі [9].

В [10] автори пропонують розглядати бізнес-моделі банків в умовах цифровізації та досліджують переваги та виклики трендів цифровізації банківського сектору України від вже впроваджених до поки що малопоширених тенденцій. Останнім часом фокус уваги багатьох дослідників зосереджено на понятті кіберстійкості банків. В роботі автора [11] узагальнено теоретичні підходи щодо забезпечення кіберстійкості в сучасних вітчизняних умовах. Значна увага приділяється аналізу аналітичних досліджень авторитетних статистичних джерел, зокрема, ENISA Threat Landscape (ETL) [12-13], Verizon Data Breach Investigations Report (DBIR) [14-15], CrowdStrike Global Threat Report та інших.

Постановка задачі

Метою даного дослідження є проведення аналізу сучасних кіберзагроз фінансової сфери для встановлення актуальних та дослідження потенційних трендів загроз з метою забезпечення стійкості та безперервності діяльності, ефективного реагування на інциденти, а також відповідності вимогам національного регулювання і міжнародним стандартам. В роботі проводиться інтегрований аналіз від загальносвітових тенденцій до ландшафту кіберзагроз вітчизняного масштабу. Зазначена структурованість дозволяє створити більш цілісну аналітичну картину щодо можливостей втілення глобальних трендів в конкретні форми локального контексту.

Основна частина

Кіберзагрози фінансового сектору несуть в собі особливі наслідки, що відрізняє їх від кіберзагроз інших сфер. Насамперед, крадіжка облікових даних, платіжної інформації клієнтів дають можливість прямо чи опосередковано отримати кошти, здійснивши незаконні транзакції. Необхідність банків та фінансових установ в процесі функціональної діяльності обробляти великий масив інформації з обмеженим доступом зобов'язує дотримання чіткого виконання регуляторних вимог, зокрема, PCI DSS, ISO 27001, NIST CSF, GDPR. Порушення норм регуляторів можуть негативно вплинути на захист даних клієнтів і стати причинами великих збитків для фінансових установ у вигляді штрафів. Кіберзагрози фінансової сфери пов'язані з серйозними репутаційними наслідками.

Аналіз трендів кіберзагроз фінансового сектору дозволяє відзначити їх релевантність мотивації зловмисників. Насамперед рушійну силу окремих хакерів чи кіберзлочинних груп становить фінансова складова. В той же час це можуть бути кіберзлочинці, що діють під егідою окремих держав та використовують кібератаки як інструмент дестабілізаційного впливу загальнодержавного характеру. В цьому контексті прикладом виступають хактивісти, які організовують кібератаки на фінансові установи і керуються при цьому певними ідеологічними та політичними переконаннями.

В Україні після початку повномасштабного вторгнення з боку РФ спостерігалось значне збільшення кількості кібератак на інформаційно-комунікаційні системи об'єктів критичної інфраструктури, в тому числі і банківського сектору, що потенційно призводить до негативних чи критичних наслідків загальнодержавного характеру, за даними [16] кількість нейтралізованих атак за участю СБУ склало: 2020 – 800 кібератак, 2021 – 1400, 2022 рік 4500

© Панаско О.М., Сагун А.В., Гавриш О.С. (2025). Аналіз трендів кіберзагроз як важливий етап управління ризиками фінансового сектору. Сучасний захист інформації, 2(62), 98–106. https://doi.org/10.31673/2409-7292.2025.025553

кібератак, 2023 – 4500 кібератак. Геополітика виступає істотним фактором впливу на світову фінансову сферу. За даними ENISA Threat Landscape: Finance Sector [17] протягом періоду з січня 2023 до червня 2024 року на теренах країн ЄС фінансовий сектор зазнав піків DDoS-атак як популярної форми протесту або тиску (рис. 1), пов'язаних із геополітичними подіями та хактивізмом особливо під час вторгнення РФ в Україну. Хактивісти націлювалися на європейські банки (58% таких атак) і державні фінансові веб-ресурси (21%), спричиняючи порушення в їх роботі. Загалом протягом зазначеного періоду спостерігалась відносно стабільна кількість інцидентів з окремими щомісячними коливаннями, пов'язаними, зокрема, з DDoS-атаками на окремі країни ЄС через їх заяви на підтримку України.

Дослідженнями Enisa відзначено підвищення інтенсивності та складності DDoS-атак, що перевантажують трафік мереж для ускладнення та унеможливлення доступу користувачів до банківської інфраструктури. Фахівці відзначають появу нових технік атак, значне зростання кількості і масштабів атак. Атаки набувають комбінованого ефекту, часто поєднують в собі різні вектори дій, що обумовлюють значні перерви в роботі банківських систем, великі фінансові та серйозні репутаційні втрати.

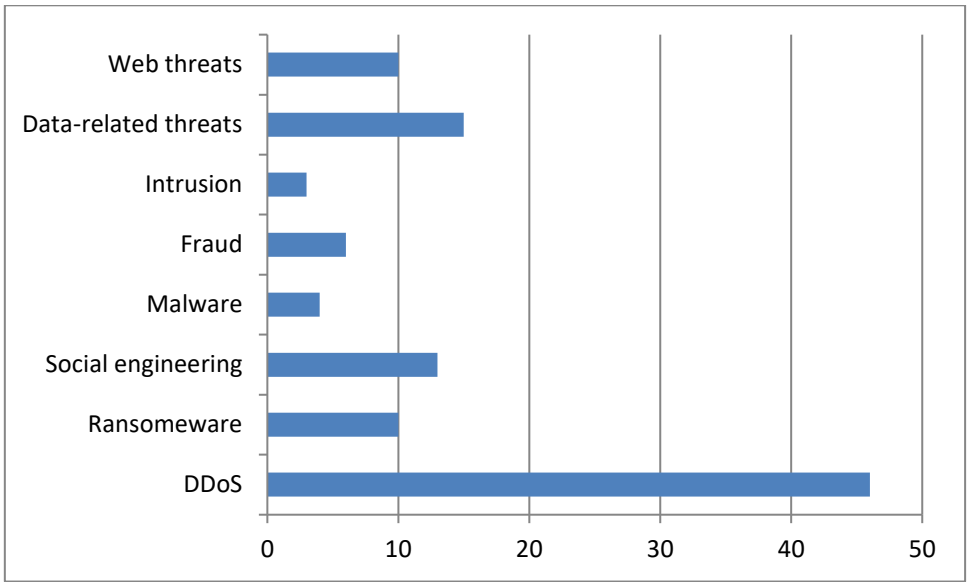

Рис.1 Загрози, що спостерігалися в європейському фінансовому секторі (січень 2023 – червень 2024)

DDoS-атаки використовуються як додаткові засоби та інструменти впливу хактивістськими або державними структурами в контексті повномасштабного вторгнення Росії в Україну, що продемонстровано потужними атаками в січні 2022 року на найбільші державні банки ПриватБанк та Ощадбанк [18], а у серпні 2024 року – на Монобанк [19].

За даними Enisa Threat Landscape 2023 та 2024 років один з основних векторів загроз для фінансового сектору був представлений атаками програм-вимагачів Ransomeware, що, зокрема, продемонстровано діяльністю таких злочинних організацій як LockBit, ALPHV (BlackCat) та Bian Lian [12-13]. Фокус уваги злочинної групи LockBit, яку за певною інформацією пов'язують з Росією, була зосереджена на атаках банків та компаній в США, Індії та Бразилії. Яскравими прикладами були масштабні кібератаки програми-вимагача Lockbit, зокрема, на Bank Syariah Indonesia в травні 2023 року, в ході якої було повністю зупинено всі служби Bank Syariah Indonesia. Внаслідок даної атаки було викрадено та оприлюднено дані користувачів [20]. Наступна подібна атака в листопаді 2023 року викликала порушення роботи систем відділу фінансових послуг Американського відділу Industrial & Commercial Bank of China, активи якого оцінюються у 23.5 млрд. доларів. LockBit провадила свою злочинну

діяльність протягом декількох років, заробляючи мільйони на зламах тисяч компаній та урядів по всьому світу, допоки в лютому 2024 року внаслідок широкомасштабної операції правоохоронних органів під керівництвом поліції Національного агентства зі злочинності Великобританії (NCA) із залученням дій української поліції не було заарештовано двох учасників угруповання Lockbit та взято під контроль інфраструктуру та систему адміністрування LockBit, а також отримано дані про членів групи [21].

Активним представником атак на фінансовий сектор виступає злочинна організація ALPHV (BlackCat або Noberus), відома застосуванням атак за допомогою програм-вимагачів на об'єкти критичної інфраструктури та інші організації. ALPHV надає можливість використовувати своє зловмисне програмне забезпечення, працюючи за моделлю Ransomware-as-a-Service, що дозволило значно розширити сфери впливу та спектр своїх жертв. Концепція тактики проведення атак програм-вимагачів зазвичай передбачає ланцюг з блокування, шифрування, видалення та крадіжки даних, але в деяких випадках ALPHV викрадають дані після отримання доступу і використовують їх для вимагання, уникаючи етап шифрування [22].

Учасники групи BianLian реалізувалися як злочинна група і здійснювали вплив на організації в різних секторах критичної інфраструктури в США, а згодом Австралії з червня 2022 року. Перші атаки BianLian використовували модель подвійного вимагання, за якою спочатку викрадалися дані, а потім шифрувалися системи жертв, а надалі вони перейшли до вимагання на основі вилучення даних. Викрадення даних жертв BianLian здійснювала через доступ до систем-жертв на основі протоколу доступу до віддаленого робочого столу через дійсні облікові дані за протоколом передачі файлів FTP, Rclone або Mega при використанні інструментів з відкритим кодом і сценарії командного рядка для виявлення та збору облікових даних.

Для банківського сектору країн ЄС спостерігалось значне зростання кількості атак та їх складності із різким збільшенням суми за викуп та підвищенням ризиків для репутації і бізнес-операцій банків [12-13], особливо з березня 2023 року. В світовому масштабі також відзначалося значне збільшення кількості атак із використанням програм-викрадачів з 2021 по 2024 рік, зокрема, якщо у 2021 році 34 відсотків фінансових організацій у всьому світі повідомили, що зазнали нападу програм-викрадачів, то в 2023 вже 64 відсотки, а в 2024 році – 65 відсотків [23].

Для заволодіння конфіденційною інформацією кіберзлочинці активно застосовують соціальну інженерію, яка в більшості випадків є ключовим механізмом початкового доступу до фінансових систем, що дозволяє зловмисникам запускати подальші етапи атаки, зокрема впровадження шкідливого ПЗ або компрометацію облікових даних. Зокрема у більшості опублікованих звітів про загрози, зокрема від ENISA та Verizon DBIR, організації та спільноти з кібербезпеки відзначають зростання складності та масштабів фішингових кампаній в фінансовій сфері як первинного вектору атак. Яскравим прикладом слугує низка фішинг-атак, організована фінансово мотивованою групою UAC-0006 у 2023 році, яка була націлена на клієнтів Приватбанку [23-24] з метою отримання несанкціонованого доступу до облікових даних клієнтів з метою заволодіння фінансовою інформацією.

Зловмисники активно використовують компрометацію ділової електронної пошти (BEC) для шахрайських дій через маніпуляцію службовою перепискою. Щоб завоювати довіру користувача та змусити його взяти участь у певній фінансовій операції, цей вид атаки застосовує різні специфічні тактики соціальної інженерії. Наприклад, у червні 2023 Microsoft виявила багатоетапну атаку AiTM (adversary-in-the-middle) із подальшою BEC-активністю, атака розпочалася з компрометації надійного постачальника та поширилася на кілька фінансових організацій. Найчастішими жертвами цих атак є працівники фінансових відділів, керівники вищої ланки та IT-персонал [25]. Упродовж останніх років шкідливе програмне забезпечення стабільно входить до переліку найпоширеніших кіберзагроз, що загрожують

фінансовому сектору, оскільки здатне проникати в банківські системи, викликаючи збої в їхній роботі та надаючи несанкціонований доступ до клієнтських даних. В травні 2024 року урядовою командою реагування на комп'ютерні інциденти CERT-UA було зафіксовано розповсюдження шкідливого програмного забезпечення SmokeLoader зловмисної організації UAC-0006. Воно використовувалося з метою формування бот-мережі для використання в системах дистанційного банківського обслуговування.

Показовим прикладом є злам Evolve Bank, який став можливим після того, як співробітник установи перейшов за посиланням шкідливого ПЗ. Це дозволило хакерам викрасти дані мільйонів клієнтів із банківських баз даних і файлових ресурсів за декілька місяців влітку 2024 року. Хакери Lockbit також вдались до атаки Evolve Bank програмами-вимагачами, внаслідок чого зловмисники заявили про отримання 650 ГБ даних клієнтів [25-26].

Кіберзлочинці дедалі частіше використовують залежність фінансового сектору від сторонніх постачальників. Атаки через треті сторони або постачальників послуг активно використовує BlackCat, що дозволяє їм проникати в системи через вразливості у взаємодії з іншими компаніями. У жовтні 2023 року LockBit було атаковано компанію Infosys McCamish Systems (IMS) – постачальника послуг для Bank of America, внаслідок чого було зашифровано понад 2 000 систем IMS та скомпрометовано дані понад 57 000 клієнтів через витік фінансових даних клієнтів [27].

Атаки нульового дня, що використовують раніше невідомі вразливості ПЗ, також становлять серйозну загрозу для фінансового сектору. Їх надзвичайно важко виявити та попередити, оскільки самі розробники часто не підозрюють про наявність таких вразливостей. У 2023 році цей тип атак набув особливої популярності, спричиняючи компрометацію критичних систем і витоки конфіденційних даних.

У ряді випадків джерелом кіберінцидентів можуть стати самі працівники фінансових установ як внаслідок навмисних дій, так і через власну необережність або незнання. Передача конфіденційної інформації чи сприяння сторонньому доступу до внутрішніх систем часто відкривають шлях для атак. У цьому контексті особливу небезпеку становлять складні, багатоетапні атаки типу Advanced Persistent Threats (APT), що здійснюються висококваліфікованими зловмисниками для встановлення несанкціонованого доступу до інфраструктури банку.

Компрометація хмарних середовищ також стає потенційною загрозою для фінансового сектору. Показовим прикладом такої компрометації став інцидент із хмарною платформою Snowflake у травні 2024 року, коли хакерське угруповування Scattered Spider здійснило масштабну атаку, використавши викрадені облікові дані клієнтів Snowflake, які не застосовували багатофакторну автентифікацію (MFA). Це дозволило зловмисникам отримати величезні масиви даних через несанкціонований доступ до облікових записів клієнтів. Серед постраждалих виявилися понад 100 організацій, включно з Santander Bank, AT&T та Ticketmaster [28].

Узагальнюючи результати аналізу, доцільно систематизувати типові кіберзагрози фінансового сектору з урахуванням особливостей їхнього прояву, причин використання та основних тенденцій поширення. Для інтерпретації природи та динаміки загроз пропонується зведена таблиця, яка інтегрує актуальні характеристики різних типів кібератак та допомагає краще зрозуміти причини використання зловмисниками тих чи інших методів у контексті фінансового сектору (табл.1).

В Україні від початку повномасштабного вторгнення фахівці сфери забезпечення кібербезпеки відзначають підвищення стійкості банків до кіберзагроз та формування сталої тенденції підвищення якості та зростання технічних можливостей для відбиття кібератак фінансового сектору, як наслідок отримання фахівцями унікального досвіду в складний час протидії інцидентам кібербезпеки [29].

Таблиця 1

Специфіка типових кіберзагроз фінансового сектору
з урахуванням особливостей їхнього прояву

Вид кібератаки	Контекст кібератаки	Причина застосування в сфері	Тенденції поширення
Ransomware	При реалізації такої загрози відбувається шифрування даних з метою вимагання викупу для відновлення, а також оприлюднення конфіденційних даних клієнтів.	Висока ймовірність того, що організації будуть готові платити за відновлення доступу до своїх даних.	Найбільш розповсюджена кіберзагроза [12-13]
Distributed Denial of Service (DDoS-атаки)	Атаки спрямовані на перевантаження інфраструктури, мережевих сервісів великою кількістю запитів для недоступності онлайн-банкінгу та інших фінансових послуг, часто супроводжуються вимаганням викупу за припинення атак, посилені геополітичними подіями.	Зупинка обробки фінансових операцій, втрата прибутків та негативні наслідки для репутації банку.	Найбільш розповсюджені [12-13]
Фішинг та соціальна інженерія	Використання різних методів для викрадення або компрометації облікових даних співробітників або клієнтів банків з метою доступу до внутрішніх систем або фінансових ресурсів	Доступ до внутрішніх систем та фінансових ресурсів, виступає основною точкою входу для зловмисників.	Тенденція до зростання порівняно з попереднім періодом [12-13].
Зловживання обліковими даними	Використання викрадених або скомпрометованих вразливих облікових даних для несанкціонованого доступу до фінансових систем.	Використовується для отримання несанкціонованого доступу до фінансових систем.	Цей вид загрози посилюється через зростання попиту на ринку викрадених даних.
Загрози постачальників	Зловмисники здійснюють атаки на фінансовий сектор через слабко захищені системи третіх сторін – постачальників або ділових партнерів, які мають доступ до інфраструктури установи.	Компрометація фінансових організацій через використання вразливостей у системах партнерів або постачальників	Атаки на ланцюги постачання були визнані суттєвими кіберзагрозами для фінансового сектору [12-13].
Зловмисне програмне забезпечення (Malware)	Використання шкідливих програм, які розповсюджуються через фішинг або інші методи соціальної інженерії.	Дана загроза передбачає спроби отримання доступу до конфіденційної інформації, викрадення коштів або компрометації банківських систем.	Зберігає тенденцію до поширеності для фінансових установ.
Атаки на хмарні сервіси	Дана загроза пов’язана з суттєвим збільшенням використання хмарних середовищ та зростанням кількості атак, спрямованих на компрометацію таких сервісів.	За дозволом НБУ після початку повномасштабного вторгнення банкам дозволено перенести власні сервіси в хмару.	У 2023 році було зафіксовано значне збільшення атак на хмарні сервіси фінансових організацій, хоча у звіті [12] цю загрозу окремо не виділяють на європейських теренах.
Інсайдерські загрози	Ненавмисні або навмисні дії співробітників, які можуть призвести до витоку інформації або компрометації систем безпеки	Незадоволені співробітники або сторонні постачальники з авторизованим доступом можуть становити значний ризик безпеки, відомий як внутрішні загрози.	Інсайдерські загрози становлять серйозну проблему, особливо в умовах зростання масштабів віддаленої роботи.

Сформована система забезпечення кібербезпеки фінансового сектору України представлена на декількох ієрархічних рівнях. Національний банк України (НБУ) уособлює її найвищий рівень та виконує завдання та функції суб'єкта національної системи захисту критичної інфраструктури, секторального органу у сфері захисту критичної інфраструктури та оператора критичної інфраструктури. В його структурі сформовано управління захисту критичної інфраструктури НБУ, а для посилення кіберзахисту банківської системи НБУ було видано постанову Правління Національного банку України від 12 серпня 2022 року №178 "Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України".

З метою організації доступу банків до системи збору, обробки, зберігання та обміну інформацією загального організаційного та технічного характеру сформовано спеціалізований сайт Національного банку, що відіграє роль інструменту для накопичення та обміну інформацією про інциденти інформаційної безпеки – MISP-NBU Центру кіберзахисту НБУ. Платформа MISP-NBU побудована на базі відкритої платформи MISP. MISP-UA гармонізована версія міжнародної платформи MISP з урахуванням специфіки вітчизняного контексту, яка сприяє ефективній реалізації обміну інформацією про кіберзагрози для фахівців, що провадять діяльність з моніторингу та реагування на кіберінциденти. Це дозволяє інтегрувати значний потенціал, набутий командами виявлення загроз та захисту систем фінансових установ та організацій, команд реагування на кіберінциденти, спеціалізованого структурного підрозділу Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України CERT.

У фінансовій сфері велике значення відіграє колективний підхід до кібербезпеки через обмін інформацією про загрози та кращі практики. Швидкий обмін інформацією про технічні деталі, індикатори компрометації, тактики, техніки і процедури дій зловмисників дають можливість проводити спільний аналіз даних, сприяють оперативній ідентифікації нових загроз та дозволяють аналізувати їх вплив на критичні інформаційні системи. MISP-UA забезпечує ефективну взаємодію між різними учасниками процесу реагування на кіберінциденти, зменшення часу реагування на кіберзагрози в фінансовій сфері, та забезпечує можливість оптимальніше підготуватися до можливих кібератак. В контексті забезпечення національної кібербезпеки MISP-UA є критично важливим інструментом, що ефективно інтегрує зусилля різних суб'єктів державного та приватного секторів у вирішальній боротьбі з кіберзагрозами.

Для забезпечення обміну інформацією про кіберзагрози ключове значення відіграє і діяльність спеціалізованих підрозділів України – Департаменту кіберполіції Національної поліції України, Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. В умовах воєнного стану особливої важливості набуває міжнародна підтримка та співпраця. В зв'язку з цим НБУ ініційовано співпрацю з Міністерством фінансів Сполучених Штатів Америки у сфері забезпечення кібербезпеки в банківському та фінансовому секторах України, що дасть змогу забезпечити підтримку ефективної системи захисту банків та фінансових установ від кіберзагроз, особливо в умовах воєнного стану, сприятиме сталому функціонуванню фінансових ринків. В цьому контексті Україна та США підписали Меморандум про співробітництво між НБУ та Міністерством фінансів США. Взаємодія між Національним банком України та Міністерством фінансів США сприятиме подальшому розвитку Центру кіберзахисту Національного банку (CSIRT NBU), а також реалізації механізмів обміну інформацією у сфері кібербезпеки та актуальних кіберзагроз.

Висновки

Аналіз трендів кіберзагроз у фінансовому секторі є вирішальним для ефективного управління ризиками кібербезпеки. Це особливо важливо для банківських установ, які

оперують не лише власними активами, а також фінансовими ресурсами клієнтів. Кібератаки можуть мати критичні наслідки, пов'язані з фінансовими втратами, витоками конфіденційної інформації, штрафами від регуляторів, а також несуть в собі довготривалі репутаційні втрати.

Постійне відстеження та розуміння потенційних кіберзагроз дозволяє не лише своєчасно реагувати на інциденти, а також впливати на кіберризики фінансових установ, вчасно запроваджуючи превентивні заходи і тим самим знижуючи ймовірність реалізації атаки. В контексті аналізу трендів кіберзагроз фінансового сектору важливе розуміння як внутрішньої ситуації, так і глобальних тенденцій.

В умовах повномасштабної війни українські банки продемонстрували помітне зростання стійкості до кібератак, набувши значного досвіду в складних умовах та зміцнивши можливості протидії інцидентам. Скоординована взаємодія державних і приватних установ відіграла в цьому важливу роль та сприяла загальному посиленню кіберзахисту фінансового сектору України.

Перелік посилань

1. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. К., 2023. №9 (вересень). 351 с.

2. Forcadell F.J., Aracil E., Ubeda F. The Impact of Corporate Sustainability and Digitalization on International Banks' Performance // Global Policy / Volume 11 (Supplement 1). pp.18-27. 2020. https://doi.org/10.1111/1758-5899.12761.

3. Карчева І. Я. Сучасні тенденції інноваційного розвитку банків України в контексті концепції банк 3.0 // Фінансовий простір. 2015. № 3(19). С. 299-305.

4. Кльоба Л. Г. Цифровізація інноваційний напрям розвитку банків // Ефективна економіка [Електронний журнал]. 2018. № 12. URL: http://www.economy.nayka.com.ua/?op=1&z=6741 (дата звернення: 10.08.2024). DOI: 10.32702/2307-2105-2018.12.84.

5. Корнівська В. О. Цифровий банкінг: ризики фінансової дигіталізації // Проблеми економіки. 2017. № 3. С. 254-261.

6. Шелудько С. А., Браткевич П. П. Вплив цифровізації на банківський бізнес в Україні // Приазовський економічний вісник. 2019. Вип. 5(16). С. 334-339. DOI: https://doi.org/10.32840/2522-4263/2019-5-57.

7. Реверчук С., Творидло О. Цифровізація банківського бізнесу: виклики та можливості для державного регулювання // Економіка та суспільство. 2023. № 55. DOI: 10.32782/2524-0072/2023-55-45.

8. Альт Р., Бек Р., Смітс М. Т. ФінТех і трансформація фінансової галузі // Електронні ринки. – 2018. – Т. 28. С. 235-243. DOI: 10.1007/s12525-018-0310-9.

9. Diener F., Špaček M. Digital Transformation in Banking: A Managerial Perspective on Barriers to Change // Sustainability. 2021. Vol. 13, No. 4. P. 2032-2058. DOI:10.3390/su13042032.

10. Кретов Д., Міндова О. Цифровізація банківського сектору України: сучасний стан та перспективи розвитку // Сталий розвиток економіки. 2024. № 2(49). С. 223–228. DOI: 10.32782/2308-1988/2024-49-35.

11. Криклій О. А. Теорія та практика забезпечення кіберстійкості банків // Ефективна економіка. 2020. № 10. URL: http://www.economy.nayka.com.ua/?op=1&z=8248. DOI: 10.32702/2307-2105-2020.10.50.

12. ENISA Threat Landscape 2024 [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024. Назва з екрана. Дата звернення: 05.03.2025.

13. ENISA Threat Landscape 2023 [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023. Назва з екрана. Дата звернення: 05.03.2025.

14. 2024 Data Breach Investigations Report [Електронний ресурс]. Режим доступу: https://www.verizon.com/business/resources/T2a8/reports/2024-dbir-data-breach-investigations-report.pdf. Назва з екрана. Дата звернення: 05.03.2025.

15. DBIR 2023 Data Breach Investigations Report [Електронний ресурс]. Режим доступу: https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf. Назва з екрана. Дата звернення: 05.03.2025.

16. Кількість кібератак на рік на критичну інфраструктуру України зросла з 800 до 4500: СБУ назвала організаторів [Електронний ресурс]. Режим доступу: https://minfin.com.ua/ua/2024/05/07/126427603/. – Назва з екрана. – Дата звернення: 15.03.2025.

17. ENISA Threat Landscape: Finance Sector [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf. Назва з екрана. Дата звернення: 09.05.2025.

18. В Україні атакували "Приватбанк", "Ощадбанк" та сайт міноборони. Атаку відбили [Електронний ресурс]. Режим доступу: https://www.bbc.com/ukrainian/news-60394077. Назва з екрана. Дата звернення: 11.03.2025.

19.Масштабна DDOS-атака на monobank припинилася [Електронний ресурс]. Режим доступу: https://forbes.ua/news/masshtabna-ddos-ataka-na-monobank-pripinilasya-19082024-23092. Назва з екрана. Дата звернення: 23.03.2025.

20. LockBit Demands $20m for 1.5TB of Data from Bank Syariah Indonesia Cyber Attack [Електронний ресурс]. Режим доступу: https://thecyberexpress.com/lockbit-bank-syariah-indonesia-cyber-attack/.Назва з екрана. Дата звернення: 12.03.2025.

21. A Global Police Operation Just Took Down the Notorious LockBit Ransomware Gang [Електронний ресурс]. Режим доступу: https://www.wired.com/story/lockbit-ransomware-takedown-website-nca-fbi/. Назва з екрана. Дата звернення: 23.03.2025.

22. ALPHV BlackCat Ransomware: A Technical Deep Dive and Mitigation Strategies [Електронний ресурс]. Режим доступу: https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/alphv-blackcat-ransomware-a-technical-deep-dive-and-mitigation-strategies/. Назва з екрана. Дата звернення: 23.03.2025.

23. Share of financial organizations worldwide hit by ransomware attacks from 2021 to 2024 [Електронний ресурс]. Режим доступу: https://www.statista.com/statistics/1460896/rate-ransomware-attacks-global/. Назва з екрана. Дата звернення: 25.03.2025.

24. Attack Methods and Payloads [Електронний ресурс]. Режим доступу: https://www.infosecurity-magazine.com/news/phishing-campaign-targets-ukraines/. Назва з екрана. Дата звернення: 15.04.2025.

25. 35% of Cybersecurity Incidents are Business Email Compromise (BEC) Phishing Attacks [Електронний ресурс]. Режим доступу: https://grsb.bank/35-of-cybersecurity-incidents-are-business-email-compromise-bec-phishing-attacks/. Назва з екрана. Дата звернення: 10.04.2025.

26. SRP Federal Credit Union reports data breach affecting more than 240,000 people [Електронний ресурс]. Режим доступу: https://www.augustachronicle.com/story/news/crime/2024/12/24/srp-federal-credit-union-announces-data-breach-to-240000-plus-people-cybersecurity-crime-nitrogen/77181661007/. Назва з екрана. Дата звернення: 17.03.2025.

27. Bank of America попереджає клієнтів про витік даних і намагається виправити ситуацію [Електронний ресурс]. Режим доступу: https: // fintechinsider.com.ua/bank-of-america-poperedzhaye-kliyentiv-pro-vytik-danyh-i-namagayetsya-vypravyty-sytuacziyu/. Назва з екрана. Дата звернення: 23.03.2025.

28. Top 10 Biggest Cyber Attacks of 2024 & 25 Other Attacks to Know About! [Електронний ресурс]. Режим доступу: https: // www.cm-alliance.com / cybersecurity-blog / top-10-biggest-cyber-attacks-of-2024-25-other-attacks-to-know-about. Назва з екрана. Дата звернення: 09.03.2025.

29. Як українські банки захищаються від кібератак в умовах війни: розповідає Євген Балютов, директор з інформаційної безпеки Райффайзен Банку. [Електронний ресурс]. Режим доступу: https://ua.news/ua/technologies/kak-ukraynskye-banky-zashhyshhayutsya-ot-kyberatak-v-uslovyyah-vojny-rasskazyvaet-evgenyj-balyutov-dyrektor-po-ynformatsyonnoj-bezopasnosty-rajffajzen-banka. Назва з екрана. Дата звернення: 03.03.2025.

Надійшла 11.05.2025